iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

A Secure Multicast Reliability based Authenticated Routing Scheme for Data Integrity in Wireless Sensor Networks

Dr. S. Saira Banu
Department of ECS, Karpagam Academy of Higher Education y

Abstract: ***Wireless Sensor Network consists of sensor nodes where it does not depend on any infrastructure like ad hoc networks. Security is a major concern in ad hoc sensor where nodes are influenced by the internal or external attackers. In this research work, Reliable Multicast Secure Routing is established with development of secure localization model. This model consists of two steps i.e. certificate based authentication protocol and estimation of node location. Nodes are located and security is updated in all nodes. The location information about sensor nodes will not be revealed to any other third parties. The proposed protocol achieves better performance in terms of network performance metrics than previous schemes based on simulation results. Security is a major concern in Wireless Sensor networks (WMSN) where the mobile sensor nodes are easily compromised by means of several attackers. Attackers are generally divided into two types i.e. Active attacks and Passive attacks. These attacks are vulnerable to network devices and make network unavailable. Location of unknown nodes and attacks is difficult to identify in the presence of mobility period. In previous research, authors introduced schemes for the protection of location of genuine nodes from attackers. In the proposed work, network model and attack model are introduced to follow the rules of secure authentication. In second part of the protocol, secure multicast tree is formed with location integrity. This module mainly focuses on the development of secure multicast groups. In last module, public key encryption and decryption scheme is deployed to protect node from the attackers.***

Keywords: Authentication, Data integrity, location integrity, secure multicast tree, public key encryption and decryption, node authentication ratio and packet integrity.

I. INTRODUCTION

Wireless sensor networks (WSNs) comprise of motes interacting with the physical environment and collaborate among each other to provide data to the end-users. Wireless Sensor network attains more performance in proposed research protocol than existing one. Multicasting plays a major role to provide network connectivity and robustness to withstand malicious attackers. In recent years, Mobile sensor networks (MSN) have been widely used in many dynamic applications, search and rescue operations and disaster relief efforts etc. Most of the applications depend on peer to peer network collaboration. Mobile nodes are communicated in a broadcast manner through radio signals.

The communication link used in ad hoc network is broadcast. It is a unique category of multicast wherein broadcast message will be transferred from source to end node. In general, multicasting is the process of transferring messages from one node to several nodes. This routing has been widely used in many applications such as corporate audio/video conference, collaborative communications and groupware systems etc.

A single stream of data packets can be shared with many destinations and when packets are duplicated. Security protocols are required to add reliable authenticated features to the base routing protocols. Attackers are divided as active and passive. It may arise from inside or outside the network. Key management scheme is the basic block of secure routing protocols but it is not fit for ad hoc network where nodes can be varied with different network devices. It is required to ensure genuine members which hold authorized keys at any time.

In [1] a secure and energy-balanced routing algorithm was introduced to support wireless sensor network. This algorithm deployed the trust model that realized a distributed joint detection model with the combination of direct trust value and indirect trust value. In [2] gradient based routing and energy aware routing protocols were implemented for analyzing energy in WSN.. Ant Colony Optimization (ACO) was used to solve the issues in routing and energy consumption. In [3] power optimization algorithm over the TORA protocol was adopted to maximize the network lifetime. The lifetime of the network is increased whereas the number of messages can be delivered under the non uniform energy deployment.

II. RELATED WORK

Thejaswi & Harish [4] found a detailed review of sensor networks and secure data aggregation concept in WSN. The relationship between dat aggregation and security requirements of WSN was analyzed briefly and presented in a clear manner. Secure data aggregation was summarized at the destination. Thenral & Sikamani [5] presented Angle based Multicasting Routing Algorithm for Wireless Mesh Networks with guaranteed performance. It provides routing efficiency and minimum energy consumption during route maintenance.. Metin Ko & Ibrahim Korpeoglu [6] presented a packet traffic load based sink movement algorithm based on the distribution of packets in a given topology. This algorithm was extended based on the distance between the nodes and then packets are transmitted to obtain energy balanced algorithm. Hung & Phan Thi [7] focused on analysis of energy efficient routing algorithm based on Selection Cluster Head and Dijkstra Alogrithm. A shortest between cluster head and cluster member was determined to provide low cost communication and low power consumption.. Kai Han et.al [8] focused the first investigation on reliable data dissemination in duty cycled WSN with guaranteed performance. The main aim was to reduce the transmission power either in multicasting or broadcasting in the presence of network failures, power issues and packet allocation probability issues. Zhou et.al [9] reviewed the disadvantages of watchdog technique in previous reliable systems. They made an alternative suite of optimization methods to reduce the energy cost of above watchdog technique.

III.IMPLEMENTATION OF PROPOSED MODEL

A. *Network Model*

In topology is established which consists of routers and nodes. The routers are created to form a multicast backbone which forwards the traffic to main gateways. Neighbor nodes are connected according to mesh based multicast network structure. Location of mobile nodes is known to source and destination node. Geographical position of nodes is updated to source node. Nodes are randomly deployed and roaming as ad hoc fashion. Random waypoint mobility pattern is adopted in this proposed network model. Ad hoc network is modeled as a graph G = (K, P) where K is the set of vertices and P is the set of edges. Network consists of *n* number of mobile nodes with unique ID and integrated with Omni-directional antenna. Node is aware of its location and it is able to obtain relative distance to the intermediate nodes. Links are assumed to be bidirectional and symmetric.

B. *Establishing a Location based Multicast Routing Protocol*

In this phase, multicast tree is constructed based on the geographical position of mobile nodes. The multicast group message is added with group ID and the redundant nodes for all multicast groups will be removed from the multicast tree. Figure 1 shows the multicast tree formation. Parent nodes update their child node locations by sending Request_Join message. Routes are established from multiple source and multiple destination. If any node falls the category of high mobility, it will be isolated. In this scheme, mobility of nodes is kept small. During the construction of multicast tree, source node broadcasts Route_Join message to all neighbor nodes. Neighbor nodes i.e. child node join source node by replying Join_Reply message. The tree is formed until the target node or destination node joins. In order to avoid link breakage, node location ID is installed in routing tables of all mobile nodes. There are two tables maintained in source node. i.e. Location aware table and Packet forwarding table.

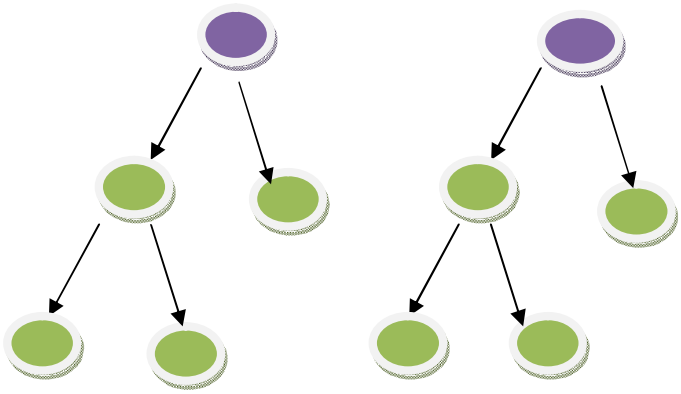


Figure 1. Illustration of Multicast tree formation

In location aware table, nodes are joined with nearest neighbor nodes based on shortest path identification and location accuracy. This location accuracy is obtained in trilateration phase. In this phase, nodes send their location with minimum spanning angle. In packet forwarding table, location status is added in header field of packet and sends with messages to nearby neighbor nodes. Child nodes intimate to its parent by updating location information. If all nodes joined together, source node decides to forward the packets towards the destination node. The relationship between child and parent node is updated based on the transmission of Child Join (CJ) and Child Leave (CL) messages.

C. Reliable Link Selection phase

In this phase, parent node finds its transmission power to forward the packets to destination node. Parent nodes periodically transmit the location aware message with maximum power that contains Parent ID and sender location information. The structure of location aware table is given below.

1) *Loc_Info:* It is the location information of sender of Request_Join message.
2) *Sour_ID:* It is the ID of source node when it is started to broadcast Request_Join message.
3) *Auth_Node:* It is the node which is authenticated by source node when its location information tracked.
4) *Link_Cate:* It is the category of link where the direction of link is bidirectional.

These fields are common in the request message whenever the source node initiates the route discovery process.

There are three possible states of nodes. i.e. Active, Monitor and Idle mode. In active mode, nodes keep on sending request message. Once the request message is expired, state will be changed to monitor.

In idle mode, node will not participate in route discovery and route maintenance process. Link connectivity is checked with intermediate nodes.

D. Public Key Encryption and Decryption Algorithm

In this phase, the concept of McEliee Public key encryption and decryption algorithm is used to protect data from the attackers. It is working on the principle of Error correcting codes.

Linear code is taken as the input to this algorithm and problem of this code is NP hard. The genuine code acts as private key and the transformed code acts as public key.

The randomization is used in the encryption process which has limited cryptanalysis. Algorithm consists of three phases. i.e. Key generation, encryption and decryption.

1) *Key Generation:* Each node should obtain a public key and its own private key.
a) *Step1:* Generate an integers as system parameters i.e. *q,m,s.*
b) *Step 2:* Each node U should follow the steps from 3 to 7.
c) *Step 3:* Select a $q \times m$ generator matrix *GM* for a binary linear code (*m,q*) to correct *e* errors.
d) *Step 4:* Choose a random $k \times k$ binary non singular matrix S.
e) *Step 5:* Select permutation matrix L.
f) *Step 6:* Find $q \times m$ matrix = SGML
g) *Step 7:* Finally U's public key is (*GM, e*) and private key is (*S,GM, L)*

2) *Encryption:* U encrypts the message *m* for V
a) *Step 1.* U find V's authenticated public key
b) *Step 2:* Message is presented as binary string with binary length *L.*
c) *Step 3:* Select a binary error vector value *x* of length *m.*
d) *Step 4:* Determine the binary vector $z = hGM + x$.
e) *Step 5:* Send the encrypted text *z* to V.

3) *Decryption:* D decrypts the cipher text and do the following.
a) *Step 1:* Determine $z' = zL^{-1}$ where L^{-1} is the inverse of L.
b) *Step 2:* Generate code by decoding cipher text to plain text.
c) *Step 3:* Find original plain text with inverse of non singular matrix.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

IV. SECURE LOCALIZATION MODEL FOR WIRELESS SENSOR NETWORKS

A. Network Model

In this phase, Mesh based routing is established between Cluster Head (CH) and cluster members to initiate packet flooding process. Once the route is established, the certificate based authentication protocol will be integrated from clusters to clusters. The following phases i.e. certificate based authentication protocol and localization model are used to secure node location information using mesh based routing.

B. Certificate based Authentication Protocol

In this phase, the concept of key pool is used to distribute the secret communication codes. Source node sends the corresponding code to the destination. The secret codes are represented as $SC_1, SC_2, ...SC_n$. Sensor nodes are categorized as mobile sensor nodes and static sensor nodes. Secret key is generated by forwarding sensor node and source sensor node.

1) *Step 1:* Reliable source node is chosen based on node reputation metric. Common Secret Code (CSC) is initialized only to reliable nodes. A secret communication link can be established by mobile sensor nodes with the help of neighbor nodes. To track the neighbor nodes, hello message will be broadcasted to all the nodes. The session key will be generated as,
2) *Step 2:* Common secret key *K* is generated between node S and D with the help of server *(W)* of S.
3) *Step 3:* The parameter E indicates below is encryption. E is a symmetric encryption algorithm. To identify replay attack, M_S, M_D are the nonces generated by S & D. The repetition of data is avoided in this case.
4) *Step 4:* The server *(W)* of S shares symmetric keys K_{ST}, K_{DT} with S, D, respectively.
5) *Step 5:* Source node S sends the plaintext to D. The encryption is done at the transmitter side of S. It is given as follows,
$$S \rightarrow D : C, S, D, E_{KSW}(M_S, C, S, D)$$
6) *Step 6:* D creates its own nonce M_D and sends it to its Server W with encrypted message and Source node message. It is as follows,
$$D \rightarrow W : C, S, D, E_{KSW}(M_S, C, S, D), E_{KDW}(M_D, C, S, D)$$
7) *Step 7:* Verifies the clear text by *W,* and generate a new key *k,* and pad it and send it to D .
$$D \leftarrow W : E_{KSW}(M_S, k), E_{KDW}(M_D, k)$$
8) *Step 8:* D decrypts the part of the message and verifies M_D, if it matches and sends the message to *S.*
$$S \leftarrow D : E_{KDW}(M_S, k)$$
9) *Step 9: D* decrypts message and checks M_D if it matched. If so, then sent a message to *S.*

C. Proposed packet format

Node ID	Hop Count	Authentication Status	Energy consumption	Path status	CRC
2	2	2	2	2	2

Figure 2 .Proposed Packet format

In figure 2. the proposed packet format is shown. Here the cluster head and cluster member ID carries 2 bytes. Third one is energy spent for suspicious node. Detection rate occupies the fourth field which updates the status of suspicious node arrival and it is reported to cluster head. Frame Check Sequence is the fifth field to denote error identification in the packet. The last filed CRC i.e. Cyclic Redundancy Check which is for error correction and detection in packet during route maintenance process.

V. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

The proposed approach is simulated with Network Simulator tool (NS 2.34). In this simulation, 100 sensor nodes move in a 1100 meter x 1100 meter square region for 100 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are given in table 1.

Table 1. RMSR simulation settings

No. of Nodes	120 nodes
Area Size	1100 X 1100 Sq.m
Mac	802.15.4
Radio Range	100m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point
Protocol	LEACH

B. Simulation Results

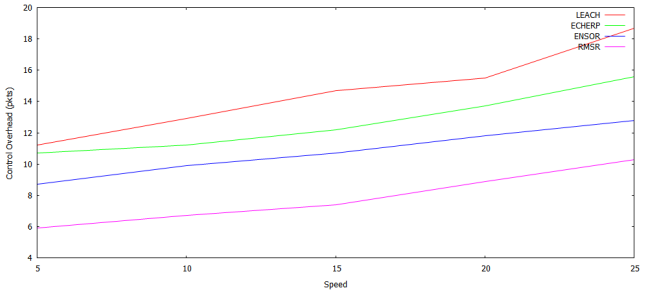


Figure 3. Control Overhead Vs Speed

Figure 3 shows the results of Overhead Vs Speed. Speed is varied as 5, 10, … 25 secs. Compared to existing schemes and protocols, the proposed protocol RMSR achieves less overhead because of mesh based routing integrated with clusters. Figure 4 show the results of packet delivery ratio while varying number of nodes from 20 to 100 nodes.. Clearly our protocol RMSR achieves more packet delivery ratio than schemes systems. The scheme comprises two major aspects i.e. reliable localization model and certificate based authentication. Packet is delivered via reliable nodes through stable link.

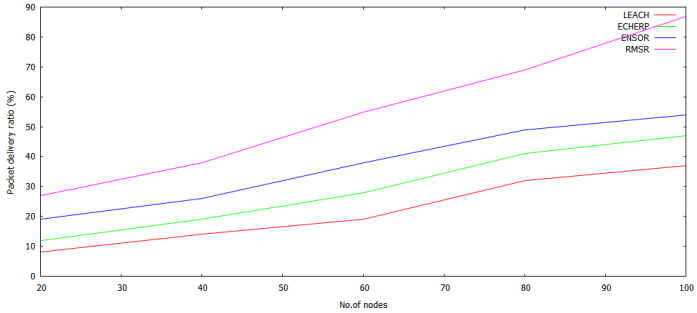


Figure 4. Packet Delivery Ratio Vs Simulation time

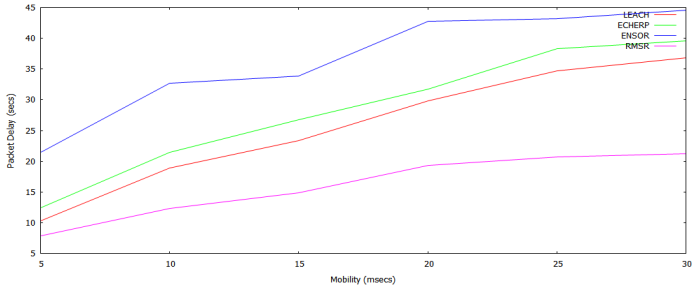


Figure 5. Packet delay Vs No. of Nodes

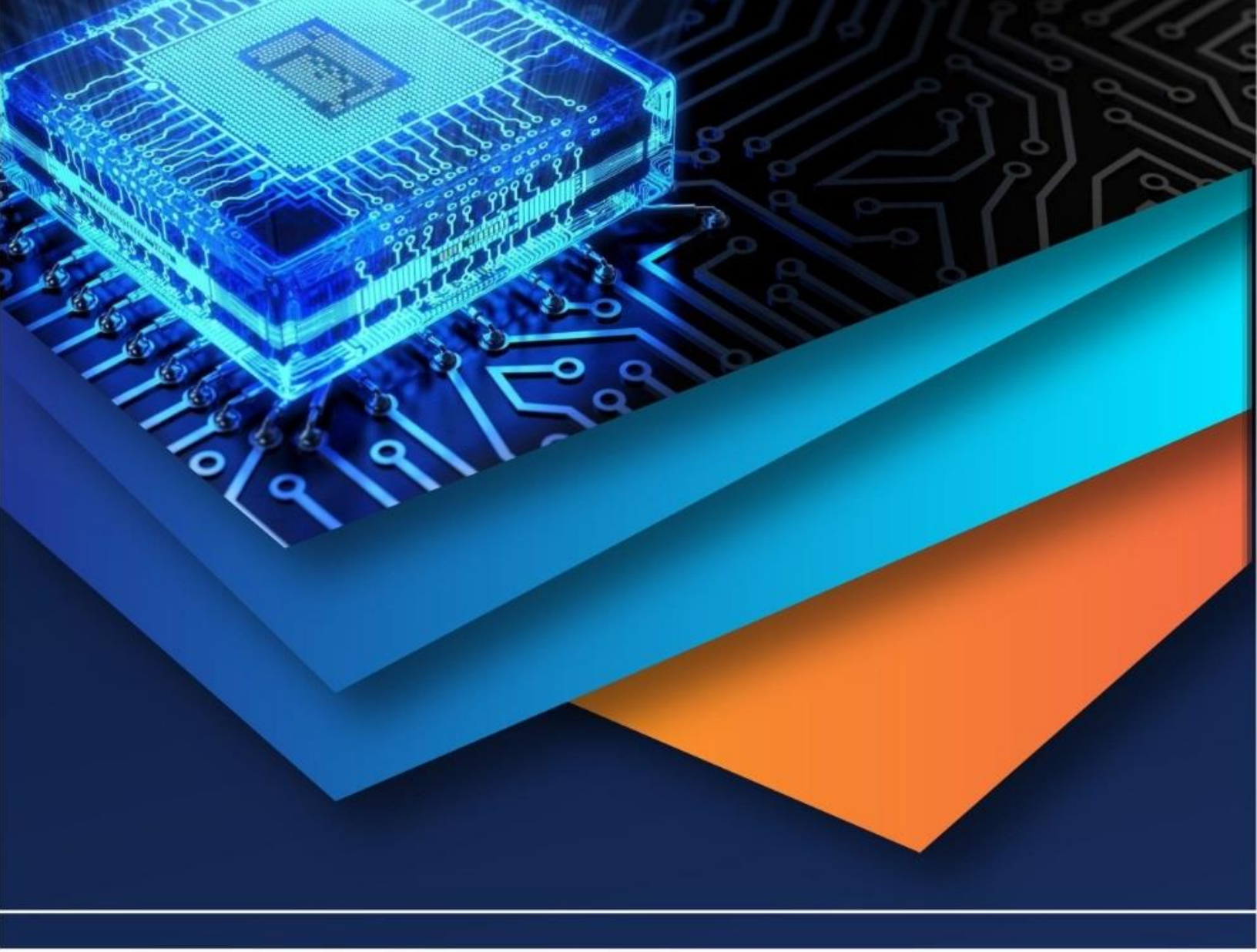
Figure 5 shows the results of Packet delay Vs Mobility. From the results, It is seen that RMSR consumes less delay than LEACH, ECHERP and ENSOR The proposed protocol reduces delay by means of mesh routing.

VI. CONCLUSION

In this research work, better performance than previous work. the node location is secured and protected from the attackers. In the presence of node mobile period, nodes are compromised by attackers and it may damage the network connectivity. Multicasting supports security and authentication in ad hoc networks. Secure multicast tree is established from the computation of location integrity and node authentication. Selection of reliable links was done in the construction phase of multicast tree. Only mesh based routing is established from parent node to child node and then destination node. If any link is making more packet loss or any node doing malfunctioning, it will be immediately identified using public key encryption and decryption technique. This technique is suitable for many applications like banking sector, online e-transfer and military areas etc.location based secure multicast routing is established from cluster head to cluster members to attain location integrity among all sensor nodes. In the presence of attackers, link reliability is difficult to adopt in the network environment. Based on the performance from simulation analysis, the proposed protocol provides better reliability and authentication. In future, it is planned to propose network ID based signcryption with certificateless routing.

REFERENCES

[1] Bei Liu, Yuanming Wu, "A Secure and Energy-Balanced Routing Scheme for Mobile Wireless Sensor Network", Wireless Sensor Network, 2015, Vol.7, pp.137-148.
[2] Rajevv Arya and S.C. Sharma, "Analysis and optimization of energy of sensor node using ACO in wireless sensor network", International Conference on Advanced Computing Technologies and Applications, Vol.45, 2015, pp.681-686.
[3] R. Saranya and R. Dhanalakshmi, "Balancing Energy Consumption to Maximize Network Lifetime Using Particle Swarm Optimization in Wireless Sensor Networks", Middle-East Journal of Scientific Research, Vol.23, 2015, pp.309-313.
[4] Thejaswi V and Harish H.K, "Secure Data Aggregation Techniques in Wireless Sensor Network", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Special Issue 5, May 2015, pp.126-131.
[5] B. Thenral **and** K. Thirunadana Sikamani, "AMRA: Angle based Multicast Routing Algorithm for Wireless Mesh Networks", Indian Journal of Science and Technology, Vol 8(13), 59451, July 2015, pp.1-8.
[6] Metin Ko and Ibrahim Korpeoglu, "Traffic- and Energy-Load based Sink Mobility Algorithms for Wireless Sensor Networks", International Journal of Sensor Networks, Vol.x, No.x, 2015, pp.1-13.
[7] Tran Cong Hung and Phan Thi The, " A Proposal to Reduce Energy Consumption for Wireless Sensor Network", Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2015 Edition, Vol. 5, No. 7,pp.1-4.
[8] Kai Han, Associate Member, IEEE, Member, ACM, Jun Luo, Member, IEEE, ACM, Liu Xiang, Mingjun Xiao, and Liusheng Huang, "Achieving Energy Efficiency and Reliability for Data Dissemination in Duty-Cycled WSNs", IEEE/ACM Transactions on networking, Vol. 23, No. 4, 2015, pp.1041-1052.
[9] Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo, "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs", IEEE transactions on information forensics and security, Vol. 10, No. 3, 2015, pp.613-625.
[10] Juan Luo, Member, IEEE, Jinyu Hu, Di Wu, Member, IEEE, and Renfa Li, Senior Member, IEEE, "Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks", IEEE transactions on industrial informatics, vol. 11, no. 1, february 2015, pp.112-121.
[11] Huseyin Ugur Yildiz, Murat Temiz, and Bulent Tavli, "Impact of Limiting Hop Count on the Lifetime of Wireless Sensor Networks", IEEE communications letters, vol. 19, no. 4, april 2015, pp.569- 572.
[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY